Advanced Telephony: DPIA – X-on (Surgery Connect)

Introduction

A data protection impact assessment (DPIA) will ensure that you identify and mitigate potential data protection risks to an acceptable level before processing data that identifies individuals (personal data).

A DPIA will also help you meet a number of data protection legal requirements including:

- Data protection by design - Privacy and data protection issues must be considered at the start, or in the design phase, of a new system, product or process, then continuously while it exists.
- Accountability - Your organisation is responsible for showing how it complies with data protection laws.
- Transparency - Personal data must be used and shared in a transparent way.
- Security - Adequate measures need to be in place to protect data. This can range from policies and procedures, to technical security measures, such as encryption of data.

DPIAs are mandatory in certain circumstances. Your organisation will need to complete a data protection impact assessment (DPIA) to cover your Advanced Telephony system in compliance with UK GDPR. This is because it is using the health and care data of a large number of people in a new or different way from that used in the previous telephony system.

A DPIA involves a risk assessment. If a high level risk remains after applying mitigations, then you must consult with the Information Commissioner's Office (ICO) for further advice before starting to collect, use or share the data. The implementation of a new Advanced Telephony system is unlikely to involve any high risk processing.

A DPIA is a live document - you must update it if there are any changes to:

- the purpose - why you are proposing to use or share personal data
- the manner - how you will use or share the data
- who is involved - the organisations using and sharing personal data

A template DPIA for GP Practices to complete for the Advanced Telephony system can be found in Annex 1. We encourage organisations to adopt this template. The template is written so that it is easy to use without needing expertise in data protection. It is the responsibility of the organisation, which is deciding on why and how the data is being used and shared (known as the controller), to ensure that the DPIA is completed appropriately.

Annex 1

Data Protection Impact Assessment (DPIA) title: Advanced Telephony

SECTION 1 - DO YOU NEED TO DO A DPIA?

1. **Do you need to do a DPIA?**

   The provision of new or updated telephony systems involves the implementation of new technology. It also involves processing personal and more sensitive data (special category) of a large number of individuals in a new or different way from that used in the previous telephony system.

   a. **Summary of how data will be used and shared**

   The GP practice will use a third party advanced telephony provider to host phone calls digitally. The service will allow for call forwarding within Primary Care Networks' (PCN) partner practices to facilitate collaborative working. Statistics for call volumes will be collected and analysed to better deploy resources. When a person calls the GP Practice, the information provided will be used to ascertain which service is most suitable for the person, such as a triage call with a GP, or a visit to the local pharmacy. Relevant information from the call will be shared with heath and care professionals. The information used and shared will vary depending on what is discussed on the call.

   The advanced telephony system will also have call recording functionality for audit purposes, complaint handling and training.

SECTION 2 - WHY DO YOU NEED THE DATA?

2. **What are the purposes for using or sharing the data?**

   We need to use personal data in order to communicate with patients over the telephone. The purpose of this processing is to improve the quality and accessibility of primary care services through better signposting to services or dealing with issues. The changes come in response to:

   - increased demand on the service
   - changes to the way primary care is delivered
   - raised public expectations regarding the availability of services

   The Advanced Telephony system is being introduced because we are looking to:

   - upgrade the digital phone system to a better one
   - support multiple incoming telephone lines

3. **What are the benefits of using or sharing the data?**

   The processing used in advanced telephony is more secure than the methods that were previously in place. The benefits of the Advanced Telephony system include:

   - Better call handling
   - Increased patient satisfaction
   - Improved ability to monitor call volumes
   - Reducing telephony costs - releasing money to potentially improve services

   Installing a new telephony system will help deliver a better service to patients because they will be able to get through to the organisation quicker. The organisation will have an audit to ensure better management. More efficient call management will be a key factor in improving the responsiveness of practice services.

SECTION 3 - WHAT DATA DO YOU WANT TO USE OR SHARE?

4. **Can you use anonymous data for your purposes? If not, explain why.**

   Put an [x] next to the one that applies.

   [ ] Yes
   [x] No
   [ ] Unsure - try to provide an explanation of what you think

   Most calls we receive are from patients requiring care and support. It is not possible to provide care and support to individuals without them being identified and their identity validated by the GP Practice. In addition, phone numbers used must be logged as part of the audit trail and so that patients can be identified and contacted.

5. **Which types of personal data do you need to use and why?**

   Put an [x] next to all that apply:

[x]	Forename	[x]	Physical description, for example height	[ ]	National insurance number
[x]	Surname	[x]	Phone number	[ ]	Other numerical identifier (specify)
[x]	Address	[x]	Email address	[ ]	Photograph / pictures of people
[x]	Postcode full	[x]	GP details	[ ]	Location data e.g.
[x]	Postcode partial	[x]	Legal representative name (personal representative)	[ ]	IP address
[x]	Date of birth	[x]	NHS number	[ ]	Other – list…
[x]	Age				
[x]	Gender				

				[ ]	None of the above

Any information communicated by callers will be transferred via the Advanced Telephony system. The system will record the phone number within the audit trail. Personal data is needed to identify the caller.

6. Data protection laws mean that some data is considered particularly sensitive. This is called special category data. Which types of special category data do you need to use or share?

Put an [x] next to all that apply.

Type of data		**Reason why this is needed (leave blank if not applicable)**
[x]	Information relating to an individual's physical or mental health or condition, for example information from health and care records	This is important to provide care, for example, a patient may call about their medication details, to receive test results or to discuss a diagnosis.
[ ]	Biometric information in order to uniquely identify an individual, for example facial recognition	
[x]	Genetic data, for example details about a DNA sample taken as part of a genetic clinical service	If a patient is part of a genetic clinical service this is relevant to the patient's care, as some conditions are inherited through genes.
[x]	Information relating to an individual's sexual life or sexual orientation	A patient may wish to disclose details about their sexual life or orientation. This may be needed as part of providing care, for example to inform a diagnosis or provide condition specific care.
[ ]	Racial or ethnic origin	
[ ]	Political opinions	
[ ]	Religious or philosophical beliefs	

[ ]	Trade union membership	
[ ]	None of the above	

7. **Who are the individuals that can be identified from the data?**

   Put an [x] next to all that apply:

   [x] Patients or service users
   [x] Staff
   [x] Wider workforce
   [x] Members of the public
   [ ] Other

8. **Where will your data come from?**

   Data used as part of the Advanced Telephony system will come from the people calling the Practice.

9. **Will you be linking any data together?**

   Put an [x] next to the one that applies

   [ ] Yes - provide an explanation below and then go to 9a
   [x] No - skip to question 10
   [ ] Unsure - try to provide an explanation of what you think then go question 9a

   a. **Will it become possible, as a result of linking data, to be able to identify individuals who were not already identifiable from the original dataset?**

      Put an [x] next to the one that applies

      [ ] Yes - provide details below
      [x] No
      [ ] Unsure - try to provide details below

SECTION 4 - WHERE WILL DATA FLOW?

10. **Describe the flows of data (if applicable)**

Information processed via the Advanced Telephony system may be accessed by:

- GP staff - clinical and non-clinical roles
- Staff within the PCN who work directly for Highfield Surgery doing clinics on specified days.

Data flow name	Going from	Going to	Data description
Patient call	Patient's phone	GP advanced telephony system	Patient makes a call to the GP practice receptionist through the phone system
Call notes	GP advanced telephony system	Electronic patient record	Receptionist enters the notes from the phone call into the patient's GP record
GP/Clinician call	GP advanced telephony system	Electronic patient record	Clinician enters notes from the phone call into the patients GP record.

11. Confirm that your organisation's information asset register (IAR) or record of processing activities (ROPA) has been updated with the flows described above.

Put an [x] next to the one that applies.

[X] Yes
[ ] No
[ ] Unsure

12. Will any data be shared outside of the UK?

X ON do not transfer any information outside the UK.

Put an [x] next to the one that applies

[ ] Yes - go to question 12a
[X] No - skip to question 13
[ ] Unsure - add as a risk in section 10 with an action to find out then skip to question 13.

a. **If yes, give details, including any safeguards or measures put in place to protect the data whilst outside of the UK.**

SECTION 5 - IS THE INTENDED USE OF THE DATA LAWFUL?

13. **Under UK General Data Protection Regulation (UK GDPR) what is your lawful basis for processing personal data?**

Put an [x] next to the one that applies

[ ] (a) **We have consent** - This must be 'freely given, specific, informed and unambiguous. You should not rely on this for individual care or research, but is likely to be needed for the use of cookies on a website.

[ ] (b) **We have a contractual obligation** - between a person and a service, such as a service user and privately funded care home.

[ ] (c) **We have a legal obligation** - the law requires us to do this, for example where NHS Digital or the courts use their powers to require the data. See Annex 2 for the most likely laws that apply when using and sharing information in health and care.

[x] (e) **We need it to perform a public task** - a public body, such as an NHS organisation or Care Quality Commissioner (CQC) registered social care organisation, is required to undertake particular activities by law. See Annex 2 for the most likely laws that apply when using and sharing information in health and care.

[ ] (f) **We have a legitimate interest** - for example, a private care provider making attempts to resolve an outstanding debt for one of its service users.

[ ] **Other**

14. **If you have indicated in question 6 that you are using special category data, what is your lawful basis under UK GDPR?**

Put an [x] next to the one that applies:

[ ] (b) **We need it to comply with our legal obligations for employment** - for example, to check a person's eligibility to work in the NHS or a local authority. See Annex 2 for the most likely laws that apply when using and sharing information in health and care.

[ ] (f) **We need it for a legal claims or judicial acts** - the information is required to exercise, enforce or defend a legal right or claim, for example a person bringing litigation against a health or care organisation

[ ] (g) **We need to comply with our legal obligations to provide information where there is a substantial public interest, with a basis in**

law - for example, setting up a system to share safeguarding information. See Annex 2 for the most likely laws that apply when using and sharing information in health and care.

[x] (h) **We need it to comply with our legal obligations to provide or manage health or social care services** - providing health and care to a person, or ensuring health and care systems function to enable care to be provided. See Annex 2 for the most likely laws that apply when using and sharing information in health and care.

[ ] (i) **We need it to comply with our legal obligations for public health** - using and sharing information is necessary to deal with threats to public health, or to take action in response to a public health emergency (such as a vaccination programme). See Annex 2 for the most likely laws that apply when using and sharing information in health and care.

[ ] (j) **We need it for archiving, research and statistics where this is in the public interest** - for example, a clinical trial for a new drug, with relevant safeguards in place for the use of the participant's health and care information. See Annex 2 for the most likely laws that apply when using and sharing information in health and care.

[ ] **Other -** please state….

15. What is your legal basis for processing health and care data under the common law duty of confidentiality?

Put an [x] next to the one that applies.

[x] **Implied consent** - it is for individual care or local clinical or care audits - skip to question 16

[ ] **Explicit consent** - a very clear and specific statement of consent - go to question 15a

[ ] **Section 251 support** - this means you have approval from the Secretary of State for Health and Care or the Health Research Authority following an application to the Confidentiality Advisory Group (CAG). CAG must be satisfied that it isn't possible or practical to seek consent. Go to question 15a

[ ] **Legal requirement** - this includes where NHS Digital has directed an organisation to share the data using its legal powers. State the legal requirement in the further information section. Go to question 15a.

[ ] **Substantial public interest** - for example to prevent or detect a serious crime or to prevent serious harm to another person. The justification to disclose must be balanced against the public interest in maintaining public confidence in health and care services. An example would be setting up a system to notify relevant organisations of safeguarding concerns. Go to question 15a.

a. Please provide further information or evidence

Provide evidence as follows depending on your selection in question 15:

- A record of the explicit consent is stored in ….
- The CAG reference number is……
- The legal requirement is
- The substantial public interest justification we are relying upon is…

SECTION 6 - HOW ARE YOU KEEPING THE DATA SECURE?

16. Are you collecting information?

Put an [x] next to the one that applies.

[x] Yes - go to question 16a
[ ] No - skip to question 17

a. How is the information being collected?

The data is only collected from the individual who has telephoned the practice.

17. Are you storing information?

Put an [x] next to the one that applies

[X] Yes - go to question 17a
[ ] No - skip to question 18

a. How will information be stored?

Put an [x] next to all that apply.

[ ] Physical storage, for example filing cabinets, archive rooms etc - provide details including whether the facility is operated by your organisation or a third party
[ ] Local organisation servers - provide details
[x] Cloud storage - provide details including whether the facility is operated by your organisation or a third party - held on UK only servers
[ ] Other - please specify

XON use a mix of open source components with their own proprietary code, all held within their own secure, co-located data centres. All of this together makes the software solution that is SurgeryConnect

Call recordings are held on XON's secure servers with quadruple site resilience

Data centres are in London and Manchester and hosted on XON's own systems and do not use any third party hosting services

18. Are you transferring information?

Put an [x] next to the one that applies.

[x] Yes - go to question 18a
[ ] No - skip to question 19 -

The purpose of the Advanced Telephony system is to transfer information between the caller and the GP practice.

a. How will information be transferred?

Voicemails left by patients wishing to cancel their appointments will be sent in audio file format to a secure NHS Email which is monitored by the Reception Manager and then files are deleted once actioned.

19. How will you ensure that information is safe and secure?

Put an [x] next to all that apply.

[x] Encryption – Secure email standard (DCB1596)
[ ] Password protection
[x] Role based access controls (RBAC) - where users only have access to the data held digitally which is needed for their role (this includes setting folder permissions)
[ ] Restricted physical access - where access to personal data is restricted to a small number of people, such as access cards or keys to a restricted area
[X] Business continuity plans
[X] Security policies [data security policy, information governance and GDPR policies]
[ ] Other

20. How will you ensure the information will not be used for any other purposes beyond those set out in question 2?

Specify the measures below which will be used to limit the purposes the data is used for.

Put an [x] next to all that apply and provide details.

[x] Contract - a legally binding contract between the GP Practice and system supplier

[x] Data processing agreement - this sets out the arrangements between a controller and processor and is legally binding
[ ] Data sharing agreement
[x] Audit – This is already in place and access to health records are monitored monthly and acted on if required.
[x] Staff training
[ ] Other

SECTION 7 - HOW LONG ARE YOU KEEPING THE DATA AND WHAT WILL HAPPEN TO IT AFTER THAT TIME?

21. How long are you planning to use the data for?

We intend to start using the system on 8th February 2024 and the contract runs until 8th February 2027.

22. How long do you intend to keep the data?

A log of all calls into, and out of, the Practice will be retained for 1 years.

The only recording of the call is kept in the standalone telephony system - this will be kept for a minimum 3 years for an adult and child.

The recording of the call will be accurately summarised into the patient's record but the recording will be kept elsewhere for 3 years in case it is needed to refer back to.

23. What will happen to the data at the end of this period?

Put an [x] next to all that apply.

[x] Secure destruction (for example by wiping hard drives where the logs (or calls if applicable) are stored, with evidence of a certificate of destruction)
Recordings are destroyed on a rolling basis once the retention period is up
[ ] Permanent preservation by transferring the data to a Place of Deposit run by the National Archives
[ ] Transfer to another organisation
[ ] Extension to retention period - with approved justification
[ ] It will be anonymised and kept
[ ] Other

SECTION 8 - HOW ARE PEOPLE'S RIGHTS AND CHOICES BEING MET?

24. How will you comply with the following data subject rights (where they apply)?

Individual right	How you will comply (or state *not applicable* if the right does not apply)	
The right to be informed The right to be informed about the collection and use of personal data.		We have assessed how we should inform individuals about the use of data for the Advanced Telephony system. We consider the communication methods below meet this obligation because Put an [x] next to all that apply. [x] Privacy notice(s) for all relevant organisations. Displayed on the website and waiting rooms. Information leaflets [x] Posters [x] Letters [ ] Emails [ ] Texts [ ] Social media campaign [ ] DPIA published (best practice rather than requirement) [x] Other – recorded message at start of call to inform callers they will be recorded [ ] Not applicable
The right of access The right to access details of data use and receive a copy of their personal information - this is commonly referred to as a subject access request.	The GP practice has a policy in place allowing for patients to access the information we hold about them, via the UK GDPR's subject access provisions. We will respond to all requests within one month of receiving the request, and if we cannot do this, we will explain to the requestor why and what next steps might be taken.	
The right to rectification The right to have inaccurate personal data rectified or completed if it is incomplete.	All patients have the right to have factually incorrect information (such as the wrong date of birth or address) about them corrected. We will amend any factually incorrect information where evidence is provided.	
The right to erasure The right to have personal data erased.	Not applicable in this circumstance as the data is being processed under UK GDPR Articles 6(1)(e) public task and 9(2)(h) the processing is necessary for medical	

	diagnosis; the provision of health or social care; or for the management of health or social care systems or services.
The right to restrict processing The right to limit how their data is used.	People can request the use of their data to be restricted in certain circumstances. These should be considered on a case-by-case basis.
The right to data portability The right to obtain and re-use their personal data.	Not applicable in this circumstance as the legal bases for processing the data are neither consent nor for the performance of a contract.
The right to object The right to object to the use and sharing of personal data.	People can object to their information being used for any purpose, and these objections will be considered on a case-by-case basis.

25. Will the national data opt-out need to be applied?

[ ] Yes
[x] No
[ ] Unsure - add as a risk in section 10 with an action to find out

26. Will any decisions be made in a purely automated way without any human involvement (automated decision making)?

Put an [x] next to the one that applies.

[ ] Yes - go to question 26a
[x] No - skip to question 27
[ ] Unsure - add as a risk in section 10 with an action to find out

a. Where the effect of the automated decision on the individual is substantial, how will you uphold an individual's right not to be subjected to a decision solely made by automated means)?

b. Are you using any special category data as part of automated decision making?

[ ] Yes
[ ] No

27. Detail any stakeholder consultation that has taken place (if applicable).

Not applicable

SECTION 9 - WHICH ORGANISATIONS ARE INVOLVED?

28. List the organisation(s) that will decide why and how the data is being used and shared (controllers).

The GP practice will be a controller.

29. List the organisation(s) that are being instructed to use or share the data (processors).

XON - The supplier providing the Advanced Telephony system will be a processor.

30. List any organisations that have been subcontracted by your processor to handle data

Not applicable

31. Explain the relationship between the organisations set out in questions 28, 29 and 30 and what activities they do

The relationship is between the supplier and the GP practice who have contracted them to provide cloud telephony services.

32. What due diligence measures and checks have been carried out on any processors used?

[x] **Data Security and Protection Toolkit (DSPT) compliance** –

DSPT - STORACALL TECHNOLOGY LTD (X-ON) (8JM42)
Standard Met 22/23

[X] **Registered with the Information Commissioner's Office (ICO)** –

Z8221333 – Data protection fee is in date.

[X] **Digital Technology Assessment Criteria (DTAC) assessment** –

PP-GDPR_ DPIA - EMIS Integration Ap

PP-GDPR_ DPIA - SurgeryConnect-190

[x] **Stated accreditations** -
X-on is ISO 27001 certified.

[X] **Data security and Cyber Essentials certification** -
Cyber Essentials Plus accredited.

[ ] **Other checks**

SECTION 10 - WHAT DATA PROTECTION RISKS ARE THERE AND WHAT MITIGATIONS WILL YOU PUT IN PLACE?

33. Complete the risk assessment table. Use the *risk scoring table to decide on the risk score.

Risk assessment table

Risk ref no.	Description	Risk score* (L x I)	Mitigations	Risk score* with mitigations applied
01	Power outage affecting GP servers leading to loss of availability of data	4	Back up generators kick in if mains systems fails	1 x 3 = 3
02	All staff are given unrestricted access to the phone system, and the data contained therein	2	Ensure that staff have access relevant to their role, by conducting a needs analysis, and putting in place technical measures to reflect this.	1 x 1 = 1
03	Unauthorised or accidental disclosure of personal data	2	Ensure staff are trained on the new system, with all activity captured in an audit trail	1 x 2 = 2
04	Unauthorised or accidental alteration of personal data	1	Ensure: ● All users are appropriately trained to use the system ● System is regularly backed up so it can be restored if necessary ● All activity is capture by a user audit trail, ideally to keystroke level	1 x 1 = 1
05	Unauthorised or accidental loss of access to, or destruction of, personal data	2	Ensure: ● Backup processes and procedures are in place to recover data ● All users are appropriately trained to use the system ● Any requests to delete data are confirmed by a senior user	1 x 1 = 1

*Risk scoring table

	Impact (I)

		Negligible (1)	Low (2)	Moderate (3)	Significant (4)	Catastrophic (5)
Likelihood (L)	Rare (1)	1	2	3	4	5
	Unlikely (2)	2	4	6	8	10
	Possible (3)	3	6	9	12	15
	Likely (4)	4	8	12	16	20
	Almost certain (5)	5	10	15	20	25

34. Detail any actions needed to mitigate any risks, who has approved the action, who owns the action, when it is due and whether it is complete.

Risk ref no.	Action needed	Action approver	Action owner	Due date	Status e.g outstanding/ complete

SECTION 11 - REVIEW AND SIGN OFF

Information Governance review:

NHS England have populated a DPIA Template with guidance to be utilised for the Advanced Telephony Programme. Your IG support service have reviewed the template and collated the information from your chosen Telephony Provider so that this information was included prior to any local risks or amendments undertaken by the GP practice as data controller. The next steps are for individual Practices to review and localise the DPIA to reflect on the process within their practice as the data controller and confirm any risks. Please ensure to amendment specifically in relation to the call recording settings you wish to undertake with your chosen supplier.

The IG recommendation is that you update and to share back with your IG service once finalised for a final IG review and Data Protection Officer consultation before go live.

Reviewer name: Heather Wilson

Reviewer job title: Caldicott Guardian - Admin

Reviewer contact details: heather.wilson33@nhs.net

Date of review: 07/07/2025

Comments:

Date for next review: July 2026

Approver name: Dr Daniel Bennett

Approver job title: GP Partner (Caldicott Guardian Lead)

Approver contact details: dr.bennett@nhs.net

Date of approval: 07/07/2025

Comments:

MLCSU IG First Review – 30/04/2024 by Bronwyn Casey (Senior Information Governance Consultant) and Lucie Jones (Senior Information Governance Officer). No comments made, recommending for DPO consultation.

DPO Review comments and signature – 08/05/2024

C. Mountford for ML/ICB DPO

Annex 2

The laws that health and care organisations rely on when using your information

Data protection laws mean that organisations must identify which law they are relying on when sharing information. For example if an organisation is sharing information because they are required by law to do so, they need to identify which law is requiring this. The following are the most likely laws that apply when using and sharing information in health and care. This list is not exhaustive.

Abortion Act 1967 and Abortion Regulations 1991
Requires that health and care staff share information with the Chief Medical Officer about abortion treatment they have provided.

Access to Health Records Act 1990
Allows access the health records of deceased people, for example to personal representatives or those who have a claim following the deceased person's death.

Care Act 2014
Defines how NHS organisations and local authorities must provide care and support to individuals, including for the management of safeguarding issues. This includes using information to assess any person who appears to require care and support.

Children Act 1989
Sets out the duties of local authorities and voluntary organisations in relation to the protection and care of children. It requires organisations that come into contact with children to cooperate and share information to safeguard children at risk of significant harm.

Control of Patient Information Regulations 2002 (COPI)
Allows information to be shared for specific reasons in relation to health and care, such as for the detection and prevention of cancer, to manage infectious diseases, such measles or COVID-19. It also allows for information to be shared where approval has been given for research or by the Secretary of State for Health and Social Care.

Coroners and Justice Act 2009
Sets out that health and care organisations must pass on information to coroners in England.

Employment Rights Act 1996
Sets out requirements for employers in relation to their employees. This includes keeping records of staff when working for them.

Equality Act 2010
Protects people from discrimination based on their age, disability, gender reassignment, pregnancy or maternity, race, religion or belief, sex, sexual orientation. Organisations may need to use this information to ensure that they are complying with their responsibilities under this Act.

Female Genital Mutilation Act 2003
Requires health and care professionals to report known cases of female genital mutilation to the police.

Fraud Act 2006
Defines fraudulent activities and how information may be shared, for example with the police, to prevent and detect fraud.

Health and Social Care Act 2008 and 2012
Sets out the structure of the health and social care system and describes the roles of different types of organisations. It sets out what they can and can't do and how they can or can't use information. It includes a duty for health and care staff to share information for individual care, unless health and organisations have a reasonable belief that you would object. In addition, health and care organisations may need to provide information to:

- The Secretary of State for Health and Social Care
- NHS England, which leads the NHS in England
- The Care Quality Commission, which inspects health and care services
- The National Institute for Health and Care Excellence (NICE), which provides national guidance and advice to improve health and care
- NHS Digital, which is the national provider of information, data and IT systems for health and social care.

Health and Social Care (Community Health and Standards) Act 2003
Allows those responsible for planning health and care services to investigate complaints about health and care organisations they have a contract with.

Health Protection (Notification) Regulations 2010)
Requires health professionals to help manage the outbreaks of infection by reporting certain contagious diseases to local authorities and to the UK Health Security Agency. The UK Health Security Agency is responsible for protecting people from the impact of infectious diseases.

Human Fertilisation and Embryology Act 1990
Requires health organisations to report information about assisted reproduction and fertility treatments to the Human Fertilisation and Embryology Authority.

Human Tissue Act 2004
Requires health organisations to report information about transplants, including adverse reactions to the Human Tissue Authority.

Inquiries Act 2005
Sets out requirements in relation to Public Inquiries, such as the UK COVID-19 Inquiry. Public Inquiries can request information from organisations to help them to complete their inquiry.

Local Government Act 1972
Sets out the responsibilities of local authorities in relation to social care including managing care records appropriately. For example, it lays out how they should be created, stored and how long they should be kept for.

NHS Act 2006
Sets out what NHS organisations can and can't do and how they can or can't use information. It allows confidential patient information to be used in specific circumstances for purposes beyond individual care. These include a limited number of approved research and planning purposes. Information can only be used where it is not possible to use information which doesn't identify you, or where seeking your explicit consent to use the information is not practical. The Act also sets out that information must be shared for the prevention and detection of fraud in the NHS.

Public Records Act 1958
Defines all records created by the NHS or local authorities as public records. This includes where organisations create records on behalf of the NHS or local authorities These records therefore need to be kept for certain periods of time, including permanently in some cases.

Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013
Requires employers to report deaths, major injuries and accidents to the Health and Safety Executive, the national regulator for workplace health and safety.

Safeguarding Vulnerable Groups Act 2006
Sets out requirements for organisations who work with vulnerable to share information and to perform pre-employment checks with the Disclosure and Barring Service (DBS), which is responsible for helping employers make safer recruitment decisions.

Statistics and Registration Service Act 2007
Allows health organisations that plan services and local authorities to receive and disclose health and care information to the Office for National Statistics (ONS). The ONS is the UK's largest independent producer of official statistics.

Terrorism Act 2000 and Terrorism Prevention and Investigation Measures Act 2011
Requires any person to share information with the police for the prevention and detection of terrorism related crimes.

The Road Traffic Act 1988
Requires any person to provide information to the police when requested to help identify a driver alleged to have committed a traffic offence.